様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成　25 年　6 月　1 日現在

機関番号：14301
研究種目：基盤研究(B)
研究期間：2008～2012
課題番号：20300028
研究課題名（和文）　HIP に基づく開放型ユビキタスネットワークアーキテクチャ

研究課題名（英文）Open Ubiquitous Network Architecture based on Host Identity Protocol

研究代表者
岡部 寿男（OKABE YASUO）
京都大学・学術情報メディアセンター・教授
研究者番号：20204018

研究成果の概要（和文）：
ブロードバンドネットワーク環境を、無線 LAN などのネットワークを介して、ネットワークの元々の設置者とは別の不特定の利用者が、本来の設置目的とは別の目的にも活用できるようにするのが、開放型ユビキタスネットワークアーキテクチャの考え方である。本研究課題では、このようなネットワークにおけるセキュリティとプライバシ、特に「いつ・だれが・どこに」居たかの位置情報に関するプライバシ(ロケーションプライバシ)の課題を、IP アドレスに代わる新しいアドレス体系として注目され IETF で標準化が進められている HIP (Host Identity Protocol)と、仮名(pseudonym)による認証連携を用いて解決した。

研究成果の概要（英文）：
“Open ubiquitous network architecture” or “open pervasive networking” is a framework in which an administrator can serve his own private network to unspecified anonymous users via temporary connection like Wi-Fi. In this research we have investigated issues on security and privacy in such networks and solve the issue on location privacy, “when, who and where”, using HIP (Host Identity Protocol), which is a new addressing scheme to replace IP address and is under standardization in IETF, and authentication and authorization federation via a pseudonym.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	3,000,000	900,000	3,900,000
2009 年度	3,000,000	900,000	3,900,000
2010 年度	3,100,000	930,000	4,030,000
2011 年度	2,600,000	780,000	3,380,000
2012 年度	2,662,300	810,000	3,472,300
総　計	14,362,300	4,320,000	18,682,300

研究分野：情報学
科研費の分科・細目：計算基盤・情報ネットワーク
キーワード:ユビキタスネットワーク、ロケーションプライバシ、ネットワークセキュリティ、
Host Identity Protocol、認証連携

１．研究開始当初の背景

ユビキタス時代においては，あらゆるモノにネットワーク機能が具備され、だれもがいたるところで自在にネットワークが使えることが期待される。そのようなネットワークが社会の隅々まで通信事業者(Internet Service Provider; ISP) によって整備されることは困難であることを踏まえ、今日一般家

庭でも当たり前になりつつあるブロードバンドネットワーク環境を、無線 LAN などのネットワークを介して、ネットワークの元々の設置者とは別の不特定の利用者が、本来の設置目的とは別の目的にも活用できるようにするのが、開放型ユビキタスネットワークアーキテクチャの考え方である。本研究課題では、このようなネットワークにおけるセキュリティとプライバシ、特に「いつ・だれが・どこに」居たかの位置情報に関するプライバシ（ロケーションプライバシ）の課題を、IP アドレスに代わる新しいアドレス体系として注目され IETF で標準化が進められている HIP (Host Identity Protocol) を用いて解決することを目的とする。

研究代表者らは、研究開始までに公衆無線 LAN サービスのアクセス認証技術について研究し、ネットワークアクセスの提供者と利用者の間に信頼関係を仮定しない安全な認証方式として、VPN (Virtual Private Network) を利用した「みあこネット」方式を提唱してきた。利用者にとっては、VPN を経由することで、通信を暗号化することによる盗聴や成りすましの懸念がなくなることによるセキュリティ面のメリット、すべての通信を VPN 経由とすることでネットワークアクセス提供者には通信の相手方が誰であるかがわからないことによるプライバシ面でのメリットがある。またネットワークアクセス提供者に取っても、利用者の通信はすべて利用者がアカウントを持つ VPN サーバを経由し、VPN サーバの IP アドレスを使って行われることで、インシデントにおいても基本的には直接の責任を負うことがなくなり、ログの管理などが不要になるメリットがある。しかしながら、みあこネット方式の欠点として、すべての通信が、利用者が信頼関係を持つ VPN サーバを経由するため、公衆無線 LAN のユビキタスネットワーク環境で期待されるような、アドホックネットワーク環境で目前の通信相手と直接通信するような状況には適合しなかった。

２．研究の目的

本研究では、IETF で標準化が進められている HIP (Host Identity Protocol) を応用することで、IP (Internet Protocol) のレベルでネットワークアクセス認証におけるプライバシの問題を解決する。HIP では、公開鍵暗号系に基づき公開鍵を Host Identifier (HI)、秘密鍵を Host Identity とし、IP アドレスに代わるホストの識別子として HI ならびにそのハッシュ値から生成される HIT (Host Identity Tag)を利用する。HIT は ORCHID (An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers; RFC4843) に基づく 128bit の識別子であり、上位プロトコルにおいては IPv6 アドレスと同等に扱われる。HI には well-known のものと anonymous のものとがあるが、well-known のものは DNS 上に公開され DNSSEC を用いて誰でも認証することができるようになっている。これらを利用し、通信をすべて HIP に基づいて行うことで、ユビキタスネットワーク環境におけるセキュリティの問題を解決するのが、本研究の第一の着眼点である。

しかしながら、HIP を単純に適用することでは、利用者や通信相手が誰であるかという情報がネットワークアクセスの提供者から秘匿できず、ネットワークの位置情報と組み合わせて、誰がいつどこでネットワークを使ったかというロケーションプライバシの保護が脆弱である。

Web サービスの分野においては、身分保証機関(Identity Provider; IdP) が提供する認証情報ならびに属性情報を元にサービス提供者(Service Provider; SP) が利用者のアクセスを認可し、またサービス提供者間でもユーザの同意に基づいてユーザ情報を共有しユーザに安全に便利なサービスを提供するための枠組みが実現されてきている。そこで本研究では、このような IdP と SP のモデルを開放型ユビキタスネットワークに適用し、ネットワークアクセスの提供者、ネットワークアクセスの利用者、および通信相手に対し、一定レベルの匿名性を保ちつつ Identity Provider がある種の身元保証を行うモデルを提案する。具体的には、Web サービスにおけるセキュリティ情報をやり取りするための XML 仕様である SAML (Security Assertion Markup Language)を前提に、認証連携によりネットワーク提供者と利用者の間で認証情報やアクセス認可情報をやり取りし、それに基づいて HI を動的に定義できるようにする。SAML を利用する枠組みのひとつである Liberty Alliance で採用されている仮名(pseudonym) の技術を利用して、名寄せによるプライバシ侵害のリスクを回避しつつ、万一の際のトレーサビリティを確保する。

３．研究の方法

ブロードバンドユビキタス時代において，様々な人間によって，様々な場所にネットワークアクセスとして無線 LAN などによるアクセスルータが多数設置されることになる。このことを大前提として，さらに，これらのインフラを，元々の設置・利用者とは別の人間が，本来の設置目的とは別の目的に活用できるようにする。本研究課題では、そのような開放型ユビキタスネットワークにおいて、セキュリティの確保とプラバシの保護を両立させる認証連携(Authentication and Authorization Federation)の技術を確立する。具体的には以下のようにして研究を進め

た。

A) **ネットワークアクセス提供者とネットワーク利用者の間の相互認証：**ユビキタス環境において自律分散型に配置されたアクセスルータを利用する場合には、ネットワークアクセスを提供する側が利用者を認証するだけでなく、ネットワークアクセスの利用者が、利用しようとするセンサの提供者を認証して、相互にセキュリティの確保を行えるようにする。

B) **ネットワークアクセス利用者の個人情報および位置情報の秘匿：**ネットワーク利用者の認証要求が含む利用者の位置に関する情報、および認証要求のデータ自体が含む利用者が誰かに関する情報を、利用者からの認証要求がアクセスルータないしはランデブーエージェントを経由して認証サーバに送られる際に、相互に秘匿するための技術を確立する。具体的には、仮名の利用により、位置に関する情報と、利用者が誰かという情報とを分離する。

４．研究成果

〔2008 年度〕

開放型ユビキタスネットワークにおいては、ネットワークアクセスの提供者と利用者の双方にとってのセキュリティの確保が重要である。初年度はまず、ネットワークアクセスの提供者と利用者との間で事前の信頼関係を仮定しない自律分散型のネットワークのセキュリティモデルを定義し、セキュリティに関する要求要件を明確化した。従来の公衆無線インターネットサービスは、大別して、事業者型モデル(ISP model)と自営型モデル(self-managed model)に分類できる。事業者型モデルは、ネットワークアクセスの提供者と利用者の間に契約に基づく事前の信頼関係があることを仮定し、それに基づいて認証を行う。一方、自営型モデルでは、ネットワークアクセスの提供者が、利用者との信頼関係の確立なしに、ネットワークを提供する。本研究では、ネットワークの設置者と利用者の間に、通信事業者と加入者の間にあるような契約関係や信頼関係を仮定することなしに、ネットワークの設置者と利用者の双方に対して、セキュリティの確保と同時にプライバシの保護を低コストで確実なものにできるモデルを自律分散型モデル(autonomous distributed model)と位置づけ、その単純な実現方式として、端末(Mobile Node)と認証サーバの間にトンネルが張られ通信相手(Corresponding Node)とは認証サーバを介して通信する方式を設計した。

並行して、HIP (Host Identity Protocol)におけるロケーションプライバシの問題を検討しその解決法を提案した。HIP ではランデブーエージェント(RA)を用いることでユーザは物理的な移動を意識することなくモバイル通信が可能になる.しかし一方で通信相手やネットワークを監視する第三者、さらに RA にユーザの位置情報を追跡される危険性を伴う。そこで BLIND フレームワークとして提案されていた方式を HIP において拡張することにより、移動透過性を失うことなく、通信相手に対しては位置情報を秘匿し、プロキシおよび通信経路上の盗聴者に対してはホストの識別情報を秘匿する仕組みを提案した。

〔2009 年度〕

前年度の要件定式化に基づき、ネットワークアクセス提供者およびセンサ利用者に対し、匿名性を保ちつつそれぞれに対して認証提供者がある種の身元保証を行うモデルを提案した。具体的には、Web サービスの標準である SAML(Security Assertion Markup Language)を前提に、開放型ユビキタスネットワークにおける認証を、身分保証機関(Identity Provider ； IdP)とサービス提供者(Service Provider ； SP)の認証連携としてモデル化し、そこで必要な認証情報のやりとりが扱えるようにした。SAML の最新版である 2.0 では、認証情報の提供を受けた複数のサービス提供者間が結託するいわゆる「名寄せ」により個人情報が意図せぬ形で漏洩することを避けるために IdP と SP の間では仮名を用いるなどの方式が提案されている。本研究ではこの技術を活用し、仮名を利用して相互にそのデータを提供しているのが誰かを直接は知りえないようなモデルを構築することで、ネットワークアクセス利用者の位置情報が秘匿されるようにする。この提案に従った仮名 ID 発行機構を、Shibboleth を用いて実装した。

提案方式は、欧州 TERENA(Trans-European Research and Education Networking)が主導する学術系国際無線 LAN ローミングの枠組みである eduroam にも応用可能であり、実装したシステムを利用しての Shibboleth 連携仮名 ID 発行サービスを国立情報学研究所と共同で提供した。

〔2010 年度〕

ロケーションプライバシ保護に関しては、Matos らによる HIP Location Privacy のフレームワークや、Ylitalo らによる BLIND をベースに、公開鍵がホストの識別子として使われるという HIP の特徴を活用し、移動用の ID と通信用の ID を分離する点を特徴とする新たな手法を提案した。提案方式では、ネットワーク間の移動を伴う IP 通信においても、すべての対象に対するロケーションプライバシの保護を可能としている。具体的には、

BLIND に対してモビリティ管理を行うための拡張プロトコルを構成し、モビリティとロケーションプライバシの両立に伴う通信効率や運用コストとのトレードオフについて検討した。

さらに、信頼できる補助ノードとしてのプロキシを誰がどのような責任で運用し誰がコスト負担するのかというサービスモデル、ビジネスモデルについて、VPN ベースの従来型のユビキタスネットワークアーキテクチャと比較しつつ、HIP を用いることによるメリットとデメリットの比較を行った。

一方、SAML 連携に関しては、単純な Web サービス型の認証機関のモデルでは、認証機関にプライバシ情報が集中し、認証機関自体の不正に対して脆弱になることから、認証機関を分散化し、複数の認証機関が手続きに基づいて合意した場合に限り、不正などに対するトレースができるようにするための検討を行った。その場合に各機関において保存すべきログおよびその管理、他機関から要求があった場合の開示の手続きなど情報セキュリティポリシー上の要求についても検討した。

〔2011 年度〕

Host Identity Protocol (HIP) の特徴を利用し誰もがネットワークをセキュアに提供するための公衆無線インターネットサービスにおいては、匿名でのサービス利用によるユーザの不正があった場合、ネットワーク管理者はユーザを追跡し特定できること（追跡可能性の確保）と、管理者が不正を行うことができずユーザが不正を行った場合に言い逃れができないようにすること（否認不能性の確保）が必要となる. 平成 23 年度は、HIP の特徴を利用し追跡可能性及び否認不能性を確保するための具体的な方法を提案し、実装した。特に、DNS (Domain Name System) のセキュリティ強化として導入が進められている DNSSEC に、本来の役割に加えて認証提供者としての機能を持たせる事を提案した。さらに必要なシステムの実装を行い、グローバルな評価環境を構築して運用して、システムが正常なパケットのみを通し不正なパケットをブロックできることを確認した。複数のアソシエーションの管理やログの出力、IPv6 環境での動作も確認した。

また、認証連携において用いる SAML (Security Assertion Markup Language) では, 認証を行う IdP(Identity Provider) と認可を行う SP(Service Provider)の二者が連携し、その間ではユーザの識別子として仮名の ID を用いることで個人情報の保護が行われる。本研究では、SP から IdP に利用者の個人情報が逆流し仮名性が失われることによる問題を一般的に指摘し、その解決方法として, IdP と SP の間で仮名の ID を更に変換する事を提案、その機構を Identifier Transformer (IdT) として提案した。SAML の標準機能である AP(Attribute Provider) を IdT に用いることで SAML の特徴を継承しつつも安全な変換ができるよう AP の２つの実装に合わせた詳細設計を行い, またそれらを比較した。また, AP の実装の１つ, ProxyIdP 方式の AP を用いた IdT の実装を行い, その評価及び考察を行った.

〔2012 年度〕

公開鍵である HI (Host Identity)ホストの識別子として使われるという HIP の特徴を利用し、HIP による通信開始時に base exchange でやりとりされる情報を、ネットワーク提供者の側で記録することで、万一のインシデントが発生しても HI を用いてユーザを特定するしくみを確立した。さらに HIP はエンドポイント間で一対一で association が確立してから通信を行うセキュリティプロトコルであるため 、経路上のネットワークでなりすましによる不正が生じないこと、すなわち通信が確かにエンドポイントによってなされたことを証明する否認不能性も確保できる。このための基地局の設定や管理のためのソフトウェアを設計し実装した。さらにこのようなネットワークを誰がどのように運用し誰がコスト負担するかのサービスモデルについても検討を行った。

一方、単純な HIP の適用では「いつ・だれが・どこに」居たのかの位置情報に関するプライバシが保護されない。そこで HI として仮名 の ID を用い、仮名 ID を、ネットワークの提供者とは別の主体が SAML 連携により提供するモデルを提案した。さらに、SAML 連携において 単純な Web サービス型の認証機関のモデルでは、認証機関にプライバシー情報が集中し、認証機関でのインシデントに対して脆弱になることから、認証機関を分散化し、複数の認証機関が手続きに基づいて合意した場合に限り不正等に対するトレースができるようにする方式を提案した。その場合に各機関において保存すべきログおよびその管理、他機関から要求があった場合の開示の手続きなど情報セキュリティポリシー上の要求要件を明確にした。 以上の考えに基づくシステムを実装し、実証実験を行った。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 8 件）

① 大平健司・山口由紀子・八槇博史・高倉弘喜・星野寛・中野博樹, インシデント対応を考慮した IPv6 ノード情報収集システムの設計と試作, 電子情報通信学会論文誌 D,査読有, Vol.J96-D No.6

pp.1483-1492, 2013

② 清水さや子・岡部寿男・吉田次郎, 一般カードを使った一時利用者向け認証システムの設計と実装, 情報処理学会論文誌コンシューマ・デバイス＆システム（CDS）,査読有, Vol.8, No.3, pp.34-45:, 2013.

③ 大平健司・岡部寿男, 複数 PA アドレス型 IPv6 マルチホーミングサイトにおける送信元アドレス依存動的経路制御, システム制御情報学会論文誌, 査読有, 第 25 巻第 9 号, pp.230-238, 2012.

④ 大神渉・古村隆明・岡部寿男, プライバシ情報逆流出に対する SAML/Shibboleth の仮名性強化手法, 電子情報通信学会技術報告, 査読なし, vol. 111, no. 321, IA2011-35, pp. 7-12, 2011.

⑤ 高橋暁弘・前田朋孝・岡部寿男, Host Identity Protocol を用いた, ユビキタスネットワークのセキュアな提供方法, 電子情報通信学会技術報告,査読なし, vol. 111, no. 321, IA2011-36, pp. 13-18, 2011.

⑥ 大平健司, 隅岡敦史, 北岡有喜, 古村隆明, 藤川賢治, 岡部寿男,公衆無線インターネット接続サービス「みあこネット」の設計と運用,電子情報通信学会論文誌, 査読有, Vol.J93-B, No.5, pp.759-768, 2010.

⑦ 古村隆明・岡部寿男・中村素典, SAML 連携を用いてロケーションプライバシを守る eduroam アカウント利用方式,電子情報通信学会技術報告,査読なし, vol. 109, no. 438, IA2009-109, pp. 153-158, 2010 年 3 月.

⑧ 前川慶司, 岡部寿男,Host Identity Protocol を用いたロケーションプライバシを有する匿名移動通信,電子情報通信学会技術報告,査読なし, vol. 108, no. 275, IA2008-43, pp.13-17, 2008.

〔学会発表〕（計１３件）

① Hiroyuki Sato, Yasuo Okabe, Motonori Nakamura, Takeshi Nishimura, Kazutsuna Yamaji, Privacy Enhancing Proxies in Attribute Release:Two Approaches, The 7th International Workshop on Middleware Architecture in the Internet (MirArch2013) (Proc. IEEE COMPSAC2013 Workshops), 査読有, 2013.

② 岡部寿男, 佐藤周行, 西村健, 山地一禎, 中村素典, 属性提供サーバに対してサービス提供サーバを秘匿する匿名化プロキシ, マルチメディア, 分散, 協調とモバイル(DICOMO2013)シンポジウム 8F-2, 査読なし, 2013.

③ Wataru Oogami, Takaaki Komura, Yasuo Okabe, Secure ID Transformation for Robust Pseudonymity against Backflow of Personal Information in SAML Federation, Proc. 2012 IEEE 36th International Conference on Computer Software and Applications Workshops (6th IEEE International Workshop on Middleware Architecture in the Internet (MidArch 2012)), 査読有, pp.64-69, 2012.

④ Akihiro Takahashi, Tomotaka Maeda, Yasuo Okabe, Design and Implementation of a Secure Public Wireless Internet Service Model Using Host Identity Protocol, The 12th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT2012), 査読有, pp.19-28, 2012.

⑤ 清水 さや子, 岡部 寿男, 吉田 次郎, 戸田 勝善, 一般カードを用いた認証システムにおけるハッシュ関数を用いた PIN コード生成方式, 第 5 回インターネットと運用技術シンポジウム, 査読なし, 2012.

⑥ 清水さや子・岡部寿男・吉田次郎, 一般カードを使った一時利用者向け認証システムの設計と実装, マルチメディア, 分散, 協調とモバイル(DICOMO2012)シンポジウム, pp.675-683, 2012.

⑦ Akihiro Takahashi, Yasuo Okabe, Providing Ubiquitous Networks Securely Using Host Identity Protocol, Asia Workshop on Future Internet Technologies (AWFIT2011) (In Conjunction with AINTEC 2011, Bangkok, Thailand), 査読有, 2011.

⑧ 高橋暁弘・前田朋孝・岡部寿男, Host Identity Protocol を用いたユビキタスネットワークのセキュアな提供方法, 平成 23 年度情報処理学会関西支部支部大会, 査読なし, F-29, 2011.

⑨ 大神渉・古村隆明・岡部寿男, プライバシ情報の逆流出に対する SAML/Shibboleth の仮名性強化手法, 平成 23 年度情報処理学会関西支部支部大会, 査読なし, F-30, 2011.

⑩ Akihiro Takahashi, Yasuo Okabe, Providing Ubiquitous Networks Securely using Host Identity Protocol (HIP), AsiaFI, 2011 Summer School, 査読なし, 2011.

⑪ Wataru Oogami, Takaaki Komura, Yasuo Okabe, Toward Robust Pseudonymity in Shibboleth/SAML Federation against Backflow of Personal Information, AsiaFI, 2011 Summer School, 査読なし,

2011.
⑫ Kenji Ohira, Yasuo Okabe, Host-Centric Site-Exit Router Selection in IPv6 Site Multihoming Environment, 1st International Workshop on Protocols and Applications with Multi-Homing Support (PAMS 2011), 査読有, pp. 696-703, 2011.
⑬ Keiji Maekawa, Yasuo Okabe, An Enhanced Location Privacy Framework with Mobility Using Host Identity Protocol, The 2009 International Symposium on Applications and the Internet (SAINT2009), 査読有, pp. 23-29, 2009.

〔その他〕
ホームページ等
http;//www.net.ist.i.kyoto-u.ac.jp/ja/

６．研究組織
(1)研究代表者
岡部 寿男 (OKABE YASUO)
京都大学・学術情報メディアセンター・教授
研究者番号：20204018
(2)研究分担者
宮崎 修一 (MIYAZAKI SHUICHI)
京都大学・学術情報メディアセンター・准教授
研究者番号：00303884
上原 哲太郎 (UEHARA TETSUTARO)
京都大学・学術情報メディアセンター・准教授
研究者番号：20273485
（～H23.9まで）
古村 隆明 (KOMURA TAKAAKI)
京都大学・学術情報メディアセンター・特定准教授
研究者番号：10373507
（～H23.3まで）
大平 健司 (OHIRA KENJI)
奈良先端科学技術大学院大学・大学院情報科学研究科・助教
研究者番号：40515326
中村 素典 (NAKAMURA MOTONORI)
国立情報学研究所・学術認証推進室・教授
研究者番号：30268156